



# UNITED STATES PATENT AND TRADEMARK OFFICE

*Handwritten mark*

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/802,485	03/09/2001	Burton S. Kaliski JR.	RSA-052	5894

7590 10/24/2006  
Eric L. Prah, Esq.  
HALE AND DORR LLP  
60 State Street  
Boston, MA 02109

EXAMINER

KLIMACH, PAULA W

ART UNIT PAPER NUMBER

2135

DATE MAILED: 10/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/802,485

Applicant(s)

KALISKI, BURTON S.

Examiner

Paula W. Klimach

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 31 July 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1,2,4-20,31,38-41 and 43-48 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,2,4-20,31,38-41 and 43-48 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

### ***Response to Amendment***

This office action is in response to amendment filed on 07/31/06. The amendment filed on 07/31/06 have been entered and made of record. Therefore, presently pending claims are 1-2, 4-20, 31, 38-41, and 43-48.

### ***Response to Arguments***

Applicant's arguments filed 07/31/06 have been fully considered but they are not persuasive because of following reasons.

Applicant argued that ElGamal teaches away from a protocol wherein the “server cannot feasibly determine the client secret or the third secret.” This is not found persuasive. The applicant does not claim the party B does not know K instead the applicant claims “server cannot feasibly determine the client secret or (emphasis added) the third secret.” Therefore since the server cannot feasibly determine the client secret then the system of Elgamal teaches the limitation “server cannot feasibly determine the client secret or the third secret.” Since the element A has a secret  $x_A$  and B has a secret  $x_B$ , wherein A and B send each other computations of their secrets so that  $x_A$  and  $x_B$  can remain secret (Section II).

The rejection is maintained.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**Claims 1-2, 4, 9-11, 14-17, 31, 38-41, 43, and 47-48,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones (5,623,637) in view of the article by Elgamal (A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms).

*In reference to claims 1, 38, and 47,* Jones discloses a multi-party system with a remote computer (server) and a host personal computer (client). The system of Jones after authenticating, provides to the client by the device the encrypted secrets (column 8 lines 2-67 in combination with column 9 lines 22-36). The encrypted secrets are capable of being decrypted using a decryption key derived from the third secret (column 9 lines 20-36). The multi-party secure computation protocol implemented between the client and the server is the only multi-party computation protocol that is implemented in generating the third secret and the decryption key derived from the third secret (Fig. 3).

Although Jones discloses a method of key distribution, Jones does not disclose a protocol wherein the client has a client secret and the server has a server secret used to compute a third secret from the client and server secret and the server cannot feasibly determine the client secret or the third secret.

Elgamal discloses a key distribution scheme wherein the part A and B compute the secret  $K_{AB}$  (page 469 column 2 lines 1-4). The party A has a secret  $x_A$  and B has a secret  $x_B$ . The party

Art Unit: 2135

A, which corresponds to the client, obtains the third secret ( $K_{AB}$ ). The party A has a secret  $x_A$  and B has a secret  $x_B$ , therefore the party A cannot determine the secret of Party B and Party B cannot determine the secret of Party A.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to distribute the key as disclosed by Elgamal in the system of Jones. One of ordinary skill in the art would have been motivated to do this because the opponent cannot reconstruct the key even when there is a security breach and one of the keys is discovered.

*In reference to claim 4*, wherein the client secret comprises at least one of a PIN, a password, and biometric information (column 8 lines 52-67).

*In reference to claim 9*, wherein the authenticating step comprises authenticating the client based on at least one of a PIN, a password, and biometric information (column 8 lines 52-67).

*In reference to claims 10*, wherein authenticating comprises authenticating the client based on a secret other than the first secret (column 8 lines 52-67).

*In reference to claim 43* Elgamal discloses a system wherein at the client, using the client secret to compute client information and then sending the client information to the server; at the server, using the client information and the server secret to compute intermediate data and sending the intermediate data to the client; and at the client, deriving the third secret from the intermediate data (page 469 paragraphs 3-4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to distribute the key as disclosed in the system of Elgamal in the system of Jones. One of ordinary skill in the art would have been motivated to do this because the opponent

Art Unit: 2135

cannot reconstruct the key even when there is a security breach and one of the keys is discovered.

*In reference to claims 2, 41, and 48* wherein the third secret is derived from the intermediate data by use of one of a key derivation function and a hash function. The polynomial is the key derivation function (Section II).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to distribute the key as disclosed by Elgamal in the system of Jones. One of ordinary skill in the art would have been motivated to do this because the opponent cannot reconstruct the key even when there is a security breach and one of the keys is discovered.

*In reference to claims 11* wherein authenticating comprises using an authentication secret derived from the third secret (column 9 lines 1-21).

*In reference to claim 14*, wherein the encrypted secrets comprise a private key of a public/private key pair used for asymmetric cryptography (Fig. 3).

*In reference to claim 15*, wherein the encrypted secrets comprise a signature key used for creating a digital signature.

Jones does not expressly disclose encrypted secrets comprise a signature key used for creating a digital signature.

However Elgamal discloses the key distribution for creating digital signatures (page 470).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to distribute the key as disclosed in Elgamal in the system of Jones. One of ordinary skill in the art would have been motivated to do this because the opponent cannot reconstruct the key even when there is a security breach and one of the keys is discovered.

*In reference to claim 16*, wherein authenticating comprises authenticating the client based on a secret other than the first secret, so that the user provides different information to access the device and access the signature key column 9 lines 1-21.

*In reference to claim 17*, The method of claim 1 wherein the encrypted secrets comprise a secret key used for symmetric cryptography (column 9 lines 49-60).

*In reference to claim 31* the method further comprising deriving the decryption key from the third secret; and decrypting the encrypted secrets using the decryption key (page 469).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to distribute the key as disclosed in Elgamal in the system of Jones. One of ordinary skill in the art would have been motivated to do this because the opponent cannot reconstruct the key even when there is a security breach and one of the keys is discovered.

*In reference to claim 39*, further comprising transmitting, to the first server by the network server, verification that the user has authenticated successfully.

Although Jones discloses the authentication of the host (client) to the remote computer (server), Jones does not disclose transmitting, to the first server by the network server, verification that the user has authenticated successfully. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to send verification to the client from the server that is the network server. One of ordinary skill in the art would have been motivated to do this because in the case that the authentication is successful, the information would be sent to the host computer, however if authentication is not successful the host computer could use the verification transmission to make corrections and try again.

*In reference to claim 40*, wherein the network server is a web server and wherein the client is a web browser. The server of Jones is a server on the network, therefore a network server. The common use of the network described by Jones (Fig. 1) is for the internet, therefore the server would be a web server and the client a browser.

**Claim 8** is rejected under 35 U.S.C. 103(a) as being unpatentable over Jones and Elgamal in view of Schneier.

*In reference to claim 8*, wherein the authenticating step comprises authenticating the client based on a time-dependent code. Jones and Elgamal do not expressly disclose the client authenticating based on a time-dependent code.

Schneier discloses the use of the timestamp during authentication (page 61). The information used during authentication is then time-dependent.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add a time stamp during authentication as in Schneier in the system disclosed by Jones. One of ordinary skill in the art would have been motivated to do this because the time stamp would prevent replay attacks.

**Claims 12-13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones and Elgamal as applied in claim 1 and further in view of Richard et al (5,922,074).

*In reference to claim 12* wherein the device comprises at least one of a file server, a directory server, a key server, a PDA, a mobile telephone, a smart card, and a desktop computer.



Jones and Elgamal do not expressly disclose the device comprising at least one of a file server, a directory server, a key server, a PDA, mobile telephone, a smart card, and a desktop computer.

Richard discloses a system that includes a directory server from which the client authenticates to gain access (Fig. 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate the client to a directory server as in Richard in the system of Jones. One of ordinary skill in the art would have been motivated to do this because the directory includes sensitive information that requires increased security.

*In reference to claim 13*, wherein the device comprises at least one secure data store, the device-requiring authentication before allowing the client access to the data store.

Although Jones discloses a system wherein the device requires authentication before allowing the client access to the data, Jones does not expressly disclose a system wherein the device comprises at least one secure data store.

Richard discloses a system wherein the client authenticates itself to a server that stores information or services (column 6 lines 21-45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate the client to a server that stores information or services as in Richard in the system of Jones. One of ordinary skill in the art would have been motivated to do this because the directory includes sensitive information that requires increased security.

**Claims 5-7, 18, and 44-46**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones and Elgamal as applied in claim 1 and further in view of Spelman et al (5,638,445).

*In reference to claims 5 and 44*, Jones and Elgamal do not disclose a blind function evaluation protocol used to derive the intermediate data from the secret data.

Spelman discloses a merchant device deriving an intermediate message from a secret message sent by the consumer. The merchant device uses blind encryption to determine the intermediate data (Fig. 1 in combination with column 6 lines 15-30).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to blind the secret data as disclosed by Spelman in the system disclosed Jones. One of ordinary skill in the art would have been motivated to do this because it would facilitate communication between devices in the case that the keys have not been exchanged yet.

*In reference to claims 6*, wherein the security of the blind function evaluation protocol is based on the problem of extracting roots modulo a composite.

Jones and Elgamal does not disclose the user of a blind function.

Spelman discloses the user of a blind encryption function wherein the evaluation protocol is based on the problem of extracting roots modulo a composite (column 6 lines 31-44).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to blind the secret data as disclosed by Spelman in the system disclosed Jones. One of ordinary skill in the art would have been motivated to do this because it would facilitate communication between devices in the case that the keys have not been exchanged yet.

*In reference to claims 7 and 45-46*, wherein the security of the blind function evaluation protocol uses discrete logarithms.

Jones and Elgamal does not disclose the user of a blind function.

Spelman discloses the user of a blind encryption function wherein the evaluation protocol uses the discrete logarithm problem (column 6 lines 31-44).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to blind the secret data as disclosed by Spelman in the system disclosed Jones. One of ordinary skill in the art would have been motivated to do this because it would facilitate communication between devices in the case that the keys have not been exchanged yet.

*In reference to claim 18*, wherein the encrypted secrets comprise at least one unit of digital currency.

Jones and Elgamal do not disclose the encrypted secrets comprising at least one unit of digital currency.

Spelman discloses the data being sent from a merchant to a merchant acquirer, therefore the information includes digital currency with visa information (Fig. 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to send digital currency as suggested by Spelman in the system disclosed Jones. One of ordinary skill in the art would have been motivated to do this because communication of currency requires enhanced security to prevent theft.

**Claims 19-20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones and Elgamal as applied to claim 43 and further in view of Brunsting et al (6,505,164).

*In reference to claim 19*, further comprising the step of verifying that the client has not exceeded a predetermined number of unsuccessful attempts to obtain the intermediate data.

Jones and Elgamal do not disclose a system that maintains a count of the number of unsuccessful attempt to authenticate a system.

Brunsting discloses a system that maintains a count of the number of unsuccessful attempts at accessing account information (Fig. 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain a count of the number of unsuccessful attempts as in Brunsting in the system of Jones. One of ordinary skill in the art would have been motivated to do this because it would increase security by monitoring the activity that may be malicious.

*In reference to claim 20*, wherein the verifying step further comprises: transmitting a challenge code to the client; and receiving the result of a cryptographic operation using the challenge code as an input and using a cryptographic key derived from the encrypted secret (Jones Fig. 2).

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2135

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

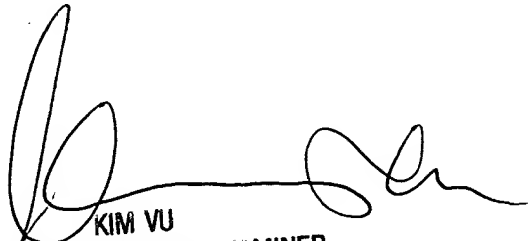
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854.

The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK  
Friday, October 13, 2006



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100